说都信息工程大学考试试卷

		Man.
	2020 — 2021 学年第 二 学期 四又19至	
	课程名称:	
	MANUAL HACHAEZ	-81
	2 2 2	
1	IV.M	
	(P)分 (D)	
UP UP	0) 1 (0) 1 (0) 2 (0) 1	
	一、単項 选择順 第9題 第10題 第11題 第12題 第13題 第14題 第15題	
100	1 11/11	
Ma	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
10 K		
料在	照答案 (
317	一、单项选择圈(每小腿 2 分,共 30 分,答案写在试卷开头相应位置处)	
補	一、中国XXX中央 1. Worm, Sasser, f 属于哪种类型的病毒?	
1993	A. 系统病毒 D. 10人	
樹山	C. 編虫病毒 D. 514234	
單, !	2. 节表中,表示节的名称的数组长度是?	
	2. 节表中, 表示 1000 年 B. 4字节 A. 5字节	
	C. 12 字节 D. 8 字节	
11)
	· · · · · · · · · · · · · · · · · · ·	
	and My Mill D. Tom s T	
	A. 3CH 子中 C. 5CH 字节 D. 6CH 字节	
		1 为
	4. 已知某节的实际大小为 290H 字节。该 PE 文件的 FileAlignmen	三 约
1 .	4. 已知某节的实际大小为 290n 子节, 则该节在内存中对齐)	

大小为: B. 300H 字节 A. 290H 字节

The state of the s			
5. PE 文件 - 照明十分解析自己属	6. 应其性代码来发示。第一个5	5.65	
展性为可读可谓。但古代妈,则英属	12.74		
A. C0000020E	8. 40000020%		
	D. A0000020h		
****		CB-91	
6. TAT 教在 PE 文件加级内存留后	Maaxxxx,	9	
和在内存中存放的信息分别是:	. 从外水水、油板油油		
A. 函数地址、函数名称	D. 展览文化、DLL 列表		
C. DLL 列表、函数名称			
7. 在一个 PE 文件中, Number Of S	action 对应的两个字句的数据	周 875年	
· · · · · · · · · · · · · · · · · · ·	410		
	- 40 10 A-T B		
A. 有 16 个节表 C. 有 16 个引入表	D. 有 10 个引出表		
8. 数据目录 DataDirectory 中岛	(本表面(结构体)占的字节是1	16 3	
	8. 6字节		
A. 5字节			
C. 7字节	0.8字节		
9. 下列哪一项内容属于引导型	山水州田林林安王龄?	()	
9. 下列哪一项内容属于引导型	病酶 布州 四 12 7 7 7 4		
A 学驻力互东第	B. 10 76 76 76 76		
C. 修改 BIOS	D. 替换 DPT 表		
10. 动态获取 API 函数地址®	t需要用到的两个函数 Load	SFIDISTA AS	
GetProcAddress,这两个函数位于	個个超块中?	()	
GetProcAddress, 这两个图数证:	B. kernel32.d11		
A. user32.d11	D. Kernerson 411		
C. cmcfg32.d11	D. netapi32.dll		
		,	1
11. 主引导扇区中的 DPT 表部	分占多少字节?	(,
11. 主引导原区中的 071 公平	B. 446 字节		
A. 445 字节			
C. 64 字节	D. 66 字节		
C. 04 7 P			
and the second s	一 那 四 粉 盐 来?	()
12. 下列哪一项不是木马自启	动常用的双小。		
16. 174 %		00.2	= -
A. DLL 劫持	D. 把木马 EXE 放在	system32 E	不下
C. 注册系统服务	D. 10 10 10 10 10 10 10 10 10 10 10 10 10		
		12.0	-
13. 木马的主要特点是隐藏,	以工工屋干太马隐藏技力	术的是?()
12 木马的主要特点是隐藏,	以下小周コルコルコルム		
13. 不可如 二人			
	- W 10 F		

		A. 油白 粉 鹹	B. 进程隐城.			
		C. 特別 2世 K/2 到底	D. 18k 35 18s ms.		3	Mil
	1		EL 9	6		4
	- 1	14. 下列不属于木马软件结构印	B. 木马服务器			18
	- 1	A. 程 號 程 字	D. 建立连接			
	1	C. 本马客户端		7)	
	- 1	15. 查看本机端口及建立连接信	息的命令是?	,		
			Mark Artists			
		A. ipconfig C. netstat	D. cmd			
		C. Herman	and the state of t	口在试验	开头相	
		二、判断圈 (对的打√, 错的打×, 每	圈 2 分,共 20 分,各条	all dr. and my		
		= Official (value)	000	war like 1	9	
Dir.	1	应位置处) 1. Windwos 平台下的动态链接库	((,d11) 文件不属于 Pt	, XTr ·	()	
101-	1	1. Windwos 平台下的观点 2. PE 文件的内存对齐粒度和文件对	齐粒度总是相等的。	Mar EL XIV	n : 10 1	
- 1	1	2. PE 文件的内存对齐粒度和文件对 3. 可以通过节的名称获取节的属性信	自息,即可以通过节的名称發	、得卫定百"	()	
	1000	写和可执行等信息。		e = 1 - 107	()	
	100	and the man to the the life OUT.	说明该表项对应的分区是常	[20] OF 12-0	1 3	
	校口	The same of the sa	MY A BA III III A A A A A A A A A A A A A	0.0	()	
M	K	5. 采用 CHS 寻址方式的设置。 6. 8086 CPU 实模式下, 最大可	寻址 1MB 的内存空间。		6 3	
数	长	7. 主引导扇区位于硬盘的 0 柱	0面1扇区。		, ,	
		7. 主引导扇区位于硬盘的 0 柱 8. 系统在启动过程中, 主引导记录:	会被 BIOS 加载到 0x7C00 的	自位置执行		
	纵	8. 紧绕在启动过程中, 主引导记录: 9. Shellcode 一般是作为数据	形式发送给服务器,制	造溢出得	以现行	
	本	9. Shellcode NETT NOT TO THE REAL PROPERTY OF THE PROPERTY OF	且各重定位的能力。		()	
	田野	代码并获取控制权的, 它不	· · · · · · · · · · · · · · · · · · ·		()	
1000	1	10. 木马可以基于 HTTP 协议建	Tribura va m			
题	1	Line of the late of the				
THE	1	三、填空题(每空1分,共10分)	HH HELDEN	c als		12
	1	三、填空題(每空1分,共10分) 1. 硬盘 CHS 寻址方式中, C表示:_		-18 XXV	-	-
	1					
	1	2. 木马入侵的基本过程是配置木马	4.		、建立连接	2.
	1	2. 木马入饺的差平过往是比量小				
		和远程控制。				
學院	1		the state of the state of	E CDU	以内友州	a tit
动		3. 系统启动时首先 BIOS 加电	自检,此时电源稳定	户, CFU	W 11 11 11	rh
	1	か 开始地	行,接卜米会特谀益。	宋) PBI 10	MDW SE	4.8.4
	1	存地址 0000:7000 处, 之)	后检查地址(WORD)000	0:	是否	等于
	1	仔地址 0000:7000 处, 之,	业上甘仙户动介质。			
	1	0xaa55, 若不等于则转去	云风共旭归例开风。			
	1			The same		
	1	4. 在 DOS 实模式下, 记录基本内	存大小的容量标志单元	的偏移是:	0000:	H
	10	4. II DOS XIXATI I IGANSIATI				

5. fs 寄存器指向当前线程的 TEB。则 fs: [30] 指向的当前进程的

四、簡答題(每小題分值见各小題,共20分)

1、手工往一个 PE 文件中插入一个新节, 需要在 PE 文件中 操作,请简略描述主要步骤及需要更改的关键信息。(本题8分》

2. 简述缓冲区溢出的基本原理。并绘制出溢出发生时栈内的变化情 况。(本题 6分)

3. 25. 支持整辑毒主要的技术手段有两个,它们分别总重定位和动态 套單 37.1 涵散建址。请简这为什么需要重定位和动态数取 AP.1 函数地址 7 《4分》写出重定位的每关汇输代码、并加以解释(4分)(本图 8分)

五、综合分析题(每小题分值见各小题,共20分)

1. 现有一 PE 文件,用文件查看工具打开的数据如下图所示,请按照 要求填空。(本题 5 分,每空 1 分)

D 0 3 6 8 9 B C Offset 00 00 00 08 97 25 37 0.9 00000000 4D 5A C1 D6 B4 BA C7 BE 67 6A 20 20 2C D1 A7 BA 00000010 00 00 30 30 FB 3A 70 69 38 29 0.0 000000020 C5 3A 67 75 6F 6A 70 65 6E 67 30 30 30 0.0 00 00000038 50 45 00 00 4C 01 00 00 55 55 55 55 30 0.0 0B 01 6E 65 6C 00000040 55 55 55 55 70 00 OF 01 6B 65 72 00 00000050 33 32 2E 64 6C 6C 00 55 88 00 00 0.0 00 0.0 0.0 000000060 00 00 00 00 00 00 40 00 04 00 00 0.0 00 0.0 04 00000070 68 C8 00 40 00 EB 03 55 04 00 68 02 40 0.0 000000080 0D 02 00 00 B8 00 00 00 6A 40 EB E4 6A 02 0.0 00000090 FF 15 EC 00 40 00 6A 0.0 FF 15 B4 00 40 0.0 55 000000A0 90 00 00 00 0D 00 00 00 55 55 55 55 55 55 55 55 000000B0 FC 00 00 00 DE 0.0 0.0 0.0 00 00 00 00 4D 65 73 73 000000C0 61 67 65 42 6F 78 41 00 4D 79 6D 69 6E 69 000000D0 45 2C 73 69 7A 65 3A 32 38 39 42 00 0.0 000000E0 45 78 69 74 50 72 6F 63 65 73 73 00 BA 00 0.0 0.0 00 00 00 00 BA 00 00 00 000000F0 EC 00 00 00 55 55 55 00 00 00 00 55 55 55 00000100 4A 00 00 00 B4 00 00 0.0 00000110 75 73 65 72 33 32 2E 64 6C 6C 00 00 10 01 00 00000120 EC 00 00 00 47 65 74 50 72 6F 63 41 64 64 72 00000130 73 73 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00000140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

(1)	PE	头	部	的	RVA	是:		
---	---	---	----	---	---	---	-----	----	--	--

(2)	该 PE	文	件中节	的	数	目	是	
-----	------	---	-----	---	---	---	---	--

14	(3) 数据目录	在文件中的偏移	是 0xA8,	则第一张导入表的	Du.
走:		第二张导入表的	RVA 是:	20 4 74 45 (II)	KYA

(4) i 文件是否存	亥 PE 文件 i 在 FOA 到 i	的内存对齐粒度是 RVA 的转换问题?	是 04H, 文件对齐	粒度是 04 _。(答"是	H。该 PE
				一。一百龙	、"否")

8

2000年 2000年

班級

送送

2. 某引导型病毒将原来硬盘的主引导组区备份至了硬盘的第 10 个扇区,同时将硬盘上的第1个扇区的内容替换成了病毒的代码。请你调用中医种程序、编写一股清除该病毒的程序代码,假设当前投寄存器 cs=ds=es=0。所程序、编写一股清除该病毒的程序代码,假设当前投寄存器 cs=ds=es=0。(int 13h 中断,相关参数的解释参考如下; AH=02H 表示选周区, AH=03H 表示写扇区; AL表示周区数; CH表示柱面; CL表示周区; DH表示磁及, DL表示图对器,值为00H*7FH为软盘;值为80H*0FFH为硬盘; ES:BX表示缓冲区的地址。) (本题 5 分,每空 0.5 分)

农 对 期 利	区的地址。)(2	K題 5 分,每空 (1) 代和	2 MOV	8.X.	-: (6)
代码 1:	MOV ax,			bx.	_; (7)
	MOV bx.	_; (2)			(8)
		2 (3)		C X .	(9)
	MOV cx.	: (4)	MOA	dx,	
	MOV dx.		Int	-:	(10)
	Int :	(5)	1110		

3. 下面是动态获取 API 函数的部分代码,请在横线上填空完善代码,相关数据结构的定义参考题后附图 (每空 1 分,共 10 分)

.code
main:
Start:

mov esi,
and esi,0fffff000h

LoopFindKernel32:
sub esi 1000h

jnz short LoopFindKernel32

GetPeHeader:

eHeader:
mov edi,dword ptr[esi+______];(3)
add edi, esi

cmp word ptr[edi],______;(4)

jnz short LoopFindKernel32

mov Kernel32Addr,esi

invoke GetApiAddress,Kernel32Addr,addr aLoadLibrary mov LoadLibraryAddr,eax

invoke GetApiAddress, Kernel32Addr, addr aGetProcAddr mov GetProcAddr, eax

invoke MessageBoxA,0,addr temp2,addr szTitle,0

invoke ExitProcess,0

mov esi,hModule add esi,[esi+3ch]

```
assume esi:ptr IMAGE_NT_HEADERS
                                          :(5)
mov esi,[esi].__
                                      ;(6)
assume esi:ptr IMAGE_EXPORT_DIRECTORY
                                            3(7)
mov ebx,[esi].
add ebx,hModule
xor edx,edx
repeat
   push esi
   mov edi,[ebx]
   add edi,hModule
   mov esi,szApiName
   mov ecx,dwApiLength
   cld
   repz empsb
   if ZERO?
        pop esi
        jmp_Find_Index
    .endif
    pop esi
    add ebx,4
                                                         :(8)
    inc edx
    .until edx >= [esi]._
    jmp_Exit
    Find Index:
        sub ebx,[esi].AddressOfNames
        sub ebx,hModule
        shr ebx.1
                                                           ;(9)
        add ebx, [esi]._
        add ebx,hModule
        movzx eax, word ptr [ebx]
        shl eax,2
                                                            ;(10)
        add eax,[esi]._
        add eax,hModule
        mov eax,[eax]
        add eax,hModule
        mov dwReturn,eax
        Exit:
```

more control delicenses met. Control delicens quality

end ream **但只要我这些的文文多书记了。** 1960707 Warranchistower. DESCRIPTION NAMED IN THE OWNER, NAMED AND Bright Labour Topics in Photo Control Sports of Size(ST)/de-Number of State Control of State of Sta STATE OF THE OWNER, WHEN THE PARTY OF THE OWNER, WHEN THE OWNE Million of Charles of Street, Special Control 100700 Santition's 180707 (Manager Room) Sectional operation 160702 NOTE: MICHELL PROPERTY. Report passer improvement with MORE Minor Species (mg/specialty) sym-MORE Mary or Consupplier to the **W**(100) Marry Interpretative and MCRC2 Machine Indianant agreement on 4000 Marchael More of DRAW, MATER, STATESTICAL DRAW, MARRIOUS, STREETING, SQUARES, STREETING, SQUARES, SQU DECREE MARKET SHALL TAMES MADE Name Control of the Owner of th COMPANY NAMED IN MADE OFFICERS, MINISTER SPECIFIC NAME OF GROOM OWNER, DESCRIPTION STATES (96(963) Spinosofficialist MARK SPINISS, MARKETT ON Siquitors.

DECK OF STREETS SEED NAME AND DESCRIPTIONS ASSESSED. 29030 Chicactecistics 296363 TimeCutaCting. WORD: Mary or The or Stone WORD 290000 PLANE DUTE OR DECKE 13300 DMCSD Name of Tax of Loss DMOKE Name of Contrast of **TMC50** MADRISOTT UNCLUME 19000 Address CCE ment 19000 Address: Charle Strain MADE EXPOSE STREET, SEC.